Article

Chinese Science Bulletin

Communication

April 2011 Vol.56 No.12: 1272–1277
doi: 10.1007/s11434-010-4049-8

Tight lower bound of consecutive lengths for QC-LDPC codes with girth at least ten

ZHANG GuoHua[1,2*], WANG JuHua[2], LI XueYuan[1] & WANG XinMei[1]

[1] *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China;*
[2] *China Academy of Space Technology (Xi'an), Xi'an 710100, China*

Received January 20, 2010; accepted April 1, 2010

For an arbitrary (3,*L*) quasi-cyclic(QC) low-density parity-check (LDPC) code with girth at least ten, a tight lower bound of the consecutive lengths is presented. For an arbitrary length above the bound the corresponding LDPC code necessarily has a girth at least ten, and for the length equal to the bound, the resultant code inevitably has a girth smaller than ten. This new conclusion can be well applied to some important issues, such as the proofs of the existence of large girth QC-LDPC codes, the construction of large girth QC-LDPC codes based on the Chinese remainder theorem, as well as the construction of LDPC codes with the guaranteed error correction capability.

low-density parity-check code, quasi-cyclic, girth, consecutive

Citation: Zhang G H, Wang J H, Li X Y, et al. Tight lower bound of consecutive lengths for QC-LDPC codes with girth at least ten. Chinese Sci Bull, 2011, 56: 1272–1277, doi: 10.1007/s11434-010-4049-8

It is widely accepted that avoiding short cycles is an important method to improve the decoding performance of low-density parity-check (LDPC) codes. As many efficient methods to delete 4-cycles and 6-cycles have been developed [1–7], how to avoid 8-cycles and even longer cycles has recently become a focus. An LDPC code is defined as the null space of a sparse matrix. If the matrix is with uniform column weight of R and uniform row weight of L, then the resultant codes are termed as (R,L)-regular. If the matrix is composed of circulant permutation matrices (CPM), then the corresponding codes are called quasi-cyclic (QC). In this paper, we denote a girth at least g by girth-g^+ and a girth equal to g by girth-g. In order to construct girth-10^+(3,L) LDPC codes, various methods are proposed from many clever ideas, such as allowing slope pairs (ASP) [8], quadratic permutation polynomial [9], balanced loops [10], government equations [11], lattice [12], 3-D cyclic lattices [13], adjacent matrix theory [14] and hill-climbing algorithm [15]. Although a large-girth code can be efficiently found by these methods, its code length is usually fixed in the sense that if the length needs to be adjusted, these algorithms must restart from scratch. An interesting technique, distinct from the above method, is to construct large-girth (3,L) codes with consecutive lengths, i.e. arbitrary integers LP, P above a certain lower bound. Recently, a type of girth-10^+(3,L) LDPC with consecutive lengths is proposed by Liu et al. [16] using the rings over finite polynomials; however, this method imposes some strict conditions on shift matrices and hence the lower bound proposed can hardly cast light on designing general girth-10^+(3,L) LDPC codes with consecutive lengths.

The main contribution of this paper is as follows. By analyzing the property of a general girth-10^+(3,L)QC-LDPC code defined by an arbitrary shift matrix, a tight lower bound of consecutive lengths is proposed. Using this shift matrix, the resulting code has a girth at least ten for arbitrary lengths above the bound, and smaller than ten for the length equal to the bound. The new bound naturally includes the recently proposed bound by [16] as a special case, and can serve as a general guideline for designing

*Corresponding author (email: zhangghcast@163.com)

girth-$10^{+}(3,L)$QC-LDPC codes with consecutive lengths.

For cryptography, many important results have been proposed during the last two decades, including the basic mathematical theory [17,18], pseudorandom sequence design [19–20], encryption system design [21–24], and cipher analysis and attack [25–28]. Since Zhou recently noted that large-girth LDPC codes would play an important role in cryptology [29], the contribution of this paper can also be well used in cryptography.

1 Tight lower bound of consecutive lengths

For a (3,*L*) QC-LDPC code with length $N=XL$, its parity-check matrix $\boldsymbol{H}_X$ can be expressed as [30]

$$\boldsymbol{H}_X=\begin{bmatrix} \boldsymbol{I}(0) & \boldsymbol{I}(0) & \cdots & \boldsymbol{I}(0) \\ \boldsymbol{I}(p_{1,0}) & \boldsymbol{I}(p_{1,1}) & \cdots & \boldsymbol{I}(p_{1,L-1}) \\ \boldsymbol{I}(p_{2,0}) & \boldsymbol{I}(p_{2,1}) & \cdots & \boldsymbol{I}(p_{2,L-1}) \end{bmatrix}, \tag{1}$$

where $\boldsymbol{I}(p)$ represents an $X\times X$ circulant permutation matrix with one at column-$(r+p)$ mod X for row-r, $0\leqslant r\leqslant X-1$, and zero elsewhere.

The shift matrix $\boldsymbol{S}$ corresponding to $\boldsymbol{H}_X$ is denoted by

$$\boldsymbol{S}=\begin{bmatrix} 0 & 0 & \cdots & 0 \\ p_{1,0} & p_{1,1} & \cdots & p_{1,L-1} \\ p_{2,0} & p_{2,1} & \cdots & p_{2,L-1} \end{bmatrix}, \tag{2}$$

where for $1\leqslant u\leqslant 2$, $1\leqslant v\leqslant$L–1 $p_{u,v}\in\{0,1,\cdots,X-1\}$ and $p_{u,0}=0$. Without loss of generality, all elements in eq. (2) are assumed to be nonnegative, since negative integers can be turned into nonnegative ones by the operation of mod X.

$\boldsymbol{H}_X$ can be uniquely determined by $\boldsymbol{S}$ and X. Let $g(\boldsymbol{H}_X)$ be the girth of $\boldsymbol{H}_X$, then we have

Lemma1: Suppose $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ for a certain integer Q. Then $g(\boldsymbol{H}_P)\geqslant 10$ for an arbitrary integer $P\geqslant 2\max\{\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D}\}+1$, where $\mathrm{A}=\max_v p_{1,v}$, $\mathrm{B}=\max_v p_{2,v}$, $\mathrm{C}=\max_v p_{2,v}-p_{1,v}$ and $\mathrm{D}=\max_v p_{1,v}-p_{2,v}$.

Proof: The idea of the proof is to show that there exist no 4-cycles, 6-cycles and 8-cycles within $\boldsymbol{H}_P$ (or equivalently within $\boldsymbol{S}$). Here are the hints. Assume that there is a t-cycle(t=4,6 or 8) within $\boldsymbol{H}_P$, then a formula holds in the modulus of P due to eq. (4) of [30]. By some basic algebraic operations, this formula is turned into a normal form such that its right-hand side (RHS) and left-hand side (LHS) are all nonnegative. Provided that P is larger than both the LHS and RHS, the formula which holds in the modulus of P also holds without the modulus. Therefore, the formula obviously holds in the modulus of an arbitrary integer, for example, Q, indicating a t-cycle within $\boldsymbol{H}_Q$, which contradicts $g(\boldsymbol{H}_Q)\geqslant 10$.

Before deriving the proof in details, we first analyse all the possible patterns of 4-,6- and 8-cycles within $\boldsymbol{S}$. From [30], a 4-cylce can only occur in any two rows of $\boldsymbol{S}$, a 6-cycle only in all the three rows of $\boldsymbol{S}$, and an 8-cycle only in either any two rows or all the three rows of $\boldsymbol{S}$.

Case A: 4–cycles

(A.1) 4-cycles in the 0th and 1st rows: Assume that there is such a 4-cycle, then there exist two integers $i\neq j$ such that

$$(0-p_{1,i})+(p_{1,j}-0)=0\ (\mathrm{mod}\,P). \tag{3}$$

Since $P>$A, the above equation becomes $p_{1,i}=p_{1,j}$. Hence,

$$(0-p_{1,i})+(p_{1,j}-0)=0\ (\mathrm{mod}\,Q). \tag{4}$$

Eq. (4) shows that there exists a 4-cycle within $\boldsymbol{H}_Q$. A contradiction.

(A.2) 4-cycles in the 0th and 2nd rows: Similarly, such cycles can not exist owing to $P>$B.

(A.3) 4-cycles in the 1st and 2nd rows: Assume that there is such a 4-cycle then there exist two integers $i\neq j$ satisfying

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})=0\ (\mathrm{mod}\,P). \tag{5}$$

As $P>\max\{2\mathrm{A},2\mathrm{B}\}\geqslant\mathrm{A}+\mathrm{B}$, eq. (5) can be simplified as

$$p_{1,i}+p_{2,j}=p_{1,j}+p_{2,i}. \tag{6}$$

Hence,

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})=0\ (\mathrm{mod}\,Q). \tag{7}$$

Eq. (7) indicates that there is a 4-cycle within $\boldsymbol{H}_Q$. A contradiction.

Case B: 6-cycles in the 0th, 1st, and 2nd rows:

Assume that there is such a 6-cycle as shown in Figure 1 (a), then there exist three integers $i,j,k(i\neq j;j\neq k;k\neq i)$ such that

$$(0-p_{1,j})+(p_{1,i}-p_{2,i})+(p_{2,k}-0)=0\ (\mathrm{mod}\,P). \tag{8}$$

Since $P>\max\{2\mathrm{A},2\mathrm{B}\}\geqslant\mathrm{A}+\mathrm{B}$, eq. (8) becomes

$$p_{1,i}+p_{2,k}=p_{1,j}+p_{2,i}. \tag{9}$$

Therefore,

$$(0-p_{1,j})+(p_{1,i}-p_{2,i})+(p_{2,k}-0)=0\ (\mathrm{mod}\,\mathrm{Q}). \tag{10}$$

Eq. (10) suggests that there is a 6-cycle with $\boldsymbol{H}_Q$, which contradicts $g(\boldsymbol{H}_Q)\geqslant 10$.

Case C: 8-cycles

(C.1):8-cycles in any two rows

(C.1.1) 8-cycles in the 0th and 1st rows: Assume that there is such an 8-cycle, and then there exist four integers $i,j,k,l(i\neq j;j\neq k;k\neq i;l\neq i)$ such that

$$(0-p_{1,i})+(p_{1,j}-0)+(0-p_{1,k})+(p_{1,l}-0)=0\ (\mathrm{mod}\,P). \tag{11}$$

As $P>2\mathrm{A}$, eq. (11) becomes

$$p_{1,j}+p_{1,l}=p_{1,i}+p_{1,k}. \tag{12}$$

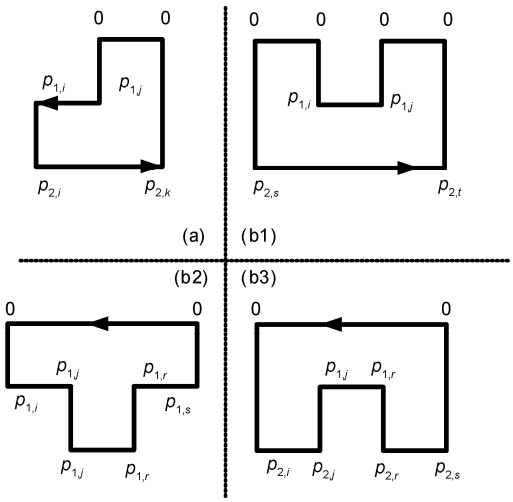

Figure 1 All possible patterns of 6-cycles and 8-cycles in all the three rows of shift matrix $\boldsymbol{S}$.

Hence,

$$(0-p_{1,i})+(p_{1,j}-0)+(0-p_{1,k})+(p_{1,l}-0)=0\,(\mathrm{mod}\,Q). \quad (13)$$

Eq. (13) shows that there is an 8-cycle in $\boldsymbol{H}_Q$. A contradiction.

(C.1.2) 8-cycles in the 0th and 2nd rows: Similarly, such cycles can not occur since P>2B.

(C.1.3) 8-cycles in the 1st and 2nd rows: Assume that there is such an 8-cycle, and then there exist four integers $i,j,k,l(i\neq j;j\neq k;k\neq l;l\neq i)$ satisfying

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})$$
$$+(p_{1,k}-p_{2,k})+(p_{2,l}-p_{1,l})=0\,(\mathrm{mod}\,P). \quad (14)$$

Define $D_x=(p_{1,x}-p_{2,x}), x\in\{i,j,k,l\}$. According to whether D_i, D_j, D_k and D_l are nonnegative or not, there are in total sixteen cases to be considered. Only six typical cases are listed below for simplicity, and the other ten cases can be proved similarly.

(C.1.3.0) $D_i\geqslant 0$, $D_j\geqslant 0$, $D_k\geqslant 0$, $D_l<0$: Since P>2D, eq. (14) becomes

$$(p_{1,i}-p_{2,i})+(p_{1,k}-p_{2,k})=(p_{1,j}-p_{2,j})+(p_{1,l}-p_{2,l}). \quad (15.0)$$

(C.1.3.1) $D_i\geqslant 0$, $D_j\geqslant 0$, $D_k<0$, $D_l<0$: As P>C+2D, eq. (14) can be simplified as

$$(p_{1,i}-p_{2,i})+(p_{1,k}-p_{2,k})+(p_{2,l}-p_{1,l})=(p_{1,j}-p_{2,j}). \quad (15.1)$$

(C.1.3.2) $D_i\geqslant 0$, $D_j<0$, $D_k<0$, $D_l<0$: Since P>C+D, eq. (14) becomes

$$(p_{1,i}-p_{2,i})+(p_{2,l}-p_{1,l})=(p_{1,j}-p_{2,j})+(p_{2,k}-p_{1,k}). \quad (15.2)$$

(C.1.3.3) $D_i\geqslant 0$, $D_j<0$, $D_k\geqslant 0$, $D_l<0$: Owing to P>2(C+D), eq. (14) can be expressed as

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})+(p_{1,k}-p_{2,k})+(p_{2,l}-p_{1,l})=0. \quad (15.3)$$

(C.1.3.4) $D_i\geqslant 0$, $D_j<0$, $D_k<0$, $D_l<0$: since P>2C+D, eq. (14) becomes

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})+(p_{2,l}-p_{1,l})=(p_{2,k}-p_{1,k}). \quad (15.4)$$

(C.1.3.5) $D_i<0$, $D_j<0$, $D_k<0$, $D_l<0$: since P>2C, eq. (14) can be reduced to

$$(p_{2,i}-p_{1,i})+(p_{2,k}-p_{1,k})=(p_{2,j}-p_{1,j})+(p_{2,l}-p_{1,l}). \quad (15.5)$$

Therefore, the following equation always holds in whatever cases.

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})+$$
$$(p_{1,k}-p_{2,k})+(p_{2,l}-p_{1,l})=0(\mathrm{mod}\,Q). \quad (16)$$

Eq. (16) implies that there is an 8-cycle in $\boldsymbol{H}_Q$. A contradiction.

(C.2):8-cycles in 0th, 1st, and 2nd rows.

Assume that there is such a cycle, then the cycle necessarily appears in one of the three patterns as shown in Figure 1(b1–b3) (for reasons see Appendix I).

(C.2.1) Assume that the 8-cycle appears as pattern (b1), then there exist four integers $i,s,t,j(i\neq s;s\neq t;t\neq j;j\neq i)$ such that

$$(p_{1,i}-0)+(0-p_{2,s})+(p_{2,t}-0)+(0-p_{1,j})=0(\mathrm{mod}\,P). \quad (17)$$

Since P>A+B, eq. (17) becomes $p_{1,i}+p_{2,t}=p_{2,s}+p_{1,j}$ and hence

$$(p_{1,i}-0)+(0-p_{2,s})+(p_{2,t}-0)+(0-p_{1,j})=0(\mathrm{mod}\,Q). \quad (18)$$

Eq. (18) shows that there is an 8-cycle in $\boldsymbol{H}_Q$. A contradiction.

(C.2.2) Assume that the 8-cycles appears as pattern (b2), then there exist four integers $i,j,r,s(i\neq j;j\neq r;r\neq s;s\neq i)$ satisfying

$$(0-p_{1,i})+(p_{1,j}-p_{2,j})+$$
$$(p_{2,r}-p_{1,r})+(p_{1,s}-0)=0(\mathrm{mod}\,P). \quad (19)$$

Define $D_x=(p_{1,x}-p_{2,x}), x\in\{j,r\}$. According to whether D_j and D_r are nonnegative or not, there are in total four cases to be considered.

(C.2.2.0) $D_j\geqslant 0$, $D_r\geqslant 0$: Since P>A+D, eq. (19) becomes

$$(p_{1,j}-p_{2,j})+p_{1,s}=p_{1,i}+(p_{1,r}-p_{2,r}), \quad (20.0)$$

(C.2.2.1) $D_j\geqslant 0$, $D_r<0$: As P>A+C+D, eq. (19) is simplified as

$$(p_{1,j}-p_{2,j})+(p_{2,r}-p_{1,r})+p_{1,s}=p_{1,i}, \quad (20.1)$$

(C.2.2.2) $D_j<0$, $D_r\geqslant 0$: since P>A+C+D, eq. (19) becomes

$$p_{1,s}=p_{1,i}+(p_{2,j}-p_{1,j})+(p_{1,r}-p_{2,r}), \quad (20.2)$$

(C.2.2.3) $D_j<0$, $D_r<0$: Due to P>A+C, eq. (19) becomes

$$(p_{2,r}-p_{1,r})+p_{1,s}=p_{1,i}+(p_{2,j}-p_{1,j}). \quad (20.3)$$

Therefore, in whatever cases we always have

$$(0-p_{1,i})+(p_{1,j}-p_{2,j})+(p_{2,r}-p_{1,r})+(p_{1,s}-0)=0(\mathrm{mod}\,Q), \quad (21)$$

Eq. (21) suggests that there is an 8-cycle in $\boldsymbol{H}_Q$. A contradiction.

(C.2.3): Similar to case (C.2.2), it is readily proved that there are no 8-cycles of pattern (b3).

By (A) to (C), $g(\boldsymbol{H}_P)\geqslant 10$ holds for arbitrary integers $P\geqslant 2\max(A,B,C+D)+1$, which completes the proof.

Q.E.D.

Remark 1: In [16] a type of girth-10$^+$(3,L)QC-LDPC codes with consecutive lengths was proposed, whose shifts matrix can be expressed as [16, eq. (5)]

$$\boldsymbol{S}=\begin{bmatrix} 0 & 0 & \cdots & 0 \\ l_0 & l_1 & \cdots & l_{L-1} \\ 3l_0 & 3l_1 & \cdots & 3l_{L-1} \end{bmatrix}. \quad (22)$$

Following the form of eq. (2), eq. (22) can be equivalently rewritten as

$$\boldsymbol{S}=\begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & l_1-l_0 & \cdots & l_{L-1}-l_0 \\ 0 & 3(l_1-l_0) & \cdots & 3(l_{L-1}-l_0) \end{bmatrix}. \quad (23)$$

Although without explicit definition, according to the proof of Theorem 2 and Table 1 in [16], $l_{L-1}-l_0$ is obviously the maximal value in the 1st line of $\boldsymbol{S}$. Therefore, A=$l_{L-1}-l_0$, B=3($l_{L-1}-l_0$), C=2($l_{L-1}-l_0$) and D=0. By lemma1, $g(\boldsymbol{H}_P)\geqslant 10$ for arbitrary integers $P\geqslant 2\times 3\times(l_{L-1}-l_0)+1$, provided $g(\boldsymbol{H}_Q)\geqslant 10$ for a certain integer Q. Thus, the lower bound discovered by [16,eq.(9)] is only a special case of lemma 1.

When $P<2\max(A,B,C+D)+1$, can $g(\boldsymbol{H}_P)\geqslant 10$ hold anymore? For the case of $P=2\max(A,B,C+D)$, we have a negative answer.

Lemma 2: $g(\boldsymbol{H}_{2\max(A,B,C+D)})<10$.

Proof: we first show that $g(\boldsymbol{H}_{2A})<10$ and $g(\boldsymbol{H}_{2B})<10$. Suppose $p_{1,x}$=A. Let P=2A then we have

$$(0-0)+(p_{1,x}-0)+(0-0)+(p_{1,x}-0)=0\ (\mathrm{mod}\,P). \quad (24)$$

Eq. (24) implies an 8-cycle in the 0th and 1st lines of $\boldsymbol{S}$, which indicates $g(\boldsymbol{H}_{2A})<10$. By similar reasoning we have $g(\boldsymbol{H}_{2B})<10$. Now consider $g(\boldsymbol{H}_{2\max(A,B,C+D)})$. Case (A): If the differences between the 2nd and 1st lines of $\boldsymbol{S}$ are all nonnegative, i.e. $p_{2,v}-p_{1,v}\geqslant 0(0\leqslant v\leqslant L-1)$, then D=0, C+D=C+0<B and hence $g(\boldsymbol{H}_{(2\max(A,B,C+D))})=g(\boldsymbol{H}_{2\max(A,B)})<10$. Case (B): If the differences between the 1st and 2nd lines of $\boldsymbol{S}$ are all nonnegative, i.e. $p_{1,v}-p_{2,v}\geqslant 0(0\leqslant v\leqslant(L-1))$, then C=0, C+D=0+D<A and hence $g(\boldsymbol{H}_{2\max(A,B,C+D)})=g(\boldsymbol{H}_{2\max(A,B)})<10$. Case (C): If the differences between the 2nd and 1st lines of $\boldsymbol{S}$ include both positive and negative integers, then obviously C and D are both positive integers. In this case, we define two nonempty sets as follows:

$\boldsymbol{X}:=\{x\mid p_{2,x}-p_{1,x}=\mathrm{C}, x\in\{0,\ldots,L-1\}\}$ and $\boldsymbol{Y}:=\{y\mid p_{1,y}-p_{2,y}=\mathrm{D}, y\in\{0,\cdots,L-1\}\}$.

In eq. (14), let $i=k\in\boldsymbol{Y}$ and $j=l\in\boldsymbol{X}$ then we have

$$\mathrm{D}+\mathrm{C}+\mathrm{D}+\mathrm{C}=0\,\mathrm{mod}(P). \quad (25)$$

For $\boldsymbol{H}_{2(C+D)}$, eq. (25) describes an 8-cycle in the 1st and 2nd lines of $\boldsymbol{S}$, which indicates that $g(\boldsymbol{H}_{2C+2D})<10$. Therefore, in case (C) we also have $g(\boldsymbol{H}_{2\max(A,B,C+D)})<10$.

Remark 2: Although $g(\boldsymbol{H}_P)\geqslant 10$ can hold for rare integers $P<2\max(A,B,C+D)$, in most cases the girth can not reach 10. In fact, by our computer computation, it seems that there is no law on the girth for this region.

From Lemmas 1 and 2, the main result of this paper can be described below.

Theorem 1: Suppose $g(\boldsymbol{H}_Q)\geqslant 10$ for a certain integer Q. Then $2L\max(A,B,C+D)$ is a tight lower bound such that $g(\boldsymbol{H}_P)\geqslant 10$ for all lengths above the bound and $g(\boldsymbol{H}_P)<10$ for the length meeting the bound, where A,B,C and D are the maximal integers of the first line, of the second line, of the difference between the second and first lines, and of the difference between the first and second lines within $\boldsymbol{S}$, respectively,

2 Some applications of the tight lower bound

2.1 Analysis of the existence of girth-10$^+$ (3,L) QC-LDPC codes

The existence problem of girth-10$^+$ (3,L) QC-LDPC codes is a very hard question in general, but Theorem 1 cast new light on this puzzle. Suppose there exists a 3×L shift matrix $\boldsymbol{S}$ such that $g(\boldsymbol{H}_Q)\geqslant 10$ for a certain integer Q, then there exist girth-10$^+$(3,L)QC-LDPC codes with arbitrary lengths $N=PL(P\geqslant 2\max\{A,B,C+D\}+1)$.

Example 1: Using a search method based on simulated annealing (developed by the authors and to be published elsewhere), we found a 3×6 shift matrix $\boldsymbol{S}$ as shown in (26). It is readily verified that $g(\boldsymbol{H}_Q)=10$ for Q=129. Since max(A,B,C+D)=B=90, according to Theorem 1, $g(\boldsymbol{H}_P)\geqslant 10$ for all the lengths $N=6P\geqslant 6(180+1)=1086$.

$$\boldsymbol{S}=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 7 & 18 & 26 \\ 0 & 10 & 24 & 44 & 77 & 90 \end{bmatrix}. \quad (26)$$

Example 2: It is easily verified that the 3×6 shift matrix $\boldsymbol{S}$ as shown in (27) ensures that $g(\boldsymbol{H}_Q)=10$ for Q=97. Since max{A,B,C+D}=C+D=134, by Theorem 1 $g(\boldsymbol{H}_P)\geqslant 10$ for all lengths $N=6P\geqslant 6(268+1)=1614$.

$$\boldsymbol{S}=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 35 & 64 & 51 & 8 & 79 \\ 0 & 96 & 73 & 90 & 94 & 31 \end{bmatrix}. \quad (27)$$

For girth-10$^+$(3,6)QC-LDPC codes, the minimal value of

consecutive lengths given by Examples 1 and 2 are 1086 and 1614, respectively, which are much smaller than that (2058) of [16]. This is because Theorem 1 does not impose any constraints on the form of shift matrices, which greatly expands the search region of the proper shift matrices.

2.2 Construction of large-girth LDPC codes by Chinese remainder theorem (CRT)

Using CRT, a longer new code can be obtained from several shorter component codes, the girth of the new code at least equal to the maximal girth of all the component codes [31]. Combined with CRT, original array codes and shorted array codes have been used as component codes to construct girth-6 and girth-8^+ QC-LDPC codes [31,32] respectively. Since the size of CPM (i.e., P) of all component codes must be coprime in the CRT method, and since P can only be prime for array codes, the two resultant types of LDPC codes are not flexible in lengths. If large-girth QC-LDPC codes with consecutive lengths were used as component codes, the CRT method will produce QC-LDPC codes with both large girth and flexible lengths. Besides, coupled with some search methods [10,14–15] for large-girth LDPC codes, Theorem 1 can readily generate many families of QC-LDPC codes with large girth as well as consecutive length. Thus, Theorem 1 has important applications in the construction of large-girth LDPC codes by the CRT method.

2.3 Construction of LDPC codes with guaranteed error correction capability (GECC)

Although LDPC codes have good error correcting properties under iterative decoding such as SPA, they generally do not have the GECC (i.e., correcting any combinations of at most n errors) as classical error-correction codes like Golay and BCH codes. Recently, a type of column weight-three LDPC codes [33] with GECC is investigated. These codes can correct any combinations of at most $g/2-1$ errors in $g/2$ iterations using Gallager-A algorithm, provided they have a girth $g \geqslant 10$. As Gallager-A algorithm is much simpler than SPA algorithm, LDPC codes with GECC will play a big role on some specific occasions. Obviously, QC-LDPC codes with GECC (4 bits) and arbitrary lengths (above a threshold) can be easily constructed with the help of Theorem 1.

3 Conclusions

A novel property of general girth-10^+ $(3,L)$ QC-LDPC codes is proposed and proved. The property states that from a given girth-$10^+(3,L)$QC-LDPC code, any $(3,L)$QC-LDPC code defined by the same shift matrix and an arbitrary size P can be obtained with a girth at least 10, provided that P is larger than a certain bound related to the shift matrix. Moreover, this bound is proved to be optimal in the sense that for P equal to the bound, the corresponding code necessarily has a girth less than 10. Finally, we would like to suggest the following problems to be further considered: (1) Investigate the three above-mentioned applications of Theorem 1. (2) "Extending" Theorem 1 to the case of girth-12 should be a meaningful problem, since QC-LDPC codes can have a girth at most 12 [30].

This work was supported by the National Basic Research Program of China (2010CB328300), the National Natural Science Foundation of China (U0635003) and "111" Project (B08038).

1 Zhang G H, Wang X M. Construction of low-density parity-check codes based on frequency-hopping sequences. Chin J El 2009, 18: 141–144
2 Zhang G H, Wang X M. Applied quasi-cyclic LDPC codes from doubly-extended RS code and cyclic MDS code (in Chinese). J Comm, 2008, 29: 100–105
3 Vasic B, Pedagani K, Ivkovic M. High-rate girth-eight low-density parity-check codes on rectangular integer lattices. IEEE Trans Comm, 2004, 52: 1248–1252
4 He S B, Zhao C M, Shi Z H, et al. Low-density parity-check codes based on sparse binary sequences (in Chinese). J Comm, 2005, 26: 81–86
5 Fujisawa M, Sakata S. A construction of high rate quasi-cyclic regular LDPC codes from cyclic difference families with girth 8. IEICE Trans Fund El Comm Comp Sci, 2007, E90-A: 1055–1061
6 Tao X F, Liu W Z, Zou X C. Construction of LDPC codes without small cycles based on geometry (in Chinese). Syst Eng El, 2007, 29: 1965–1968
7 Jing L J, Lin J L, Zhu W L. The design of structured low-density parity-check codes with large girth (in Chinese). Chin J Comp, 2007, 30: 648–654
8 Zhang H, Moura J M F. Geometry based designs of LDPC codes. In: ICC'04, Paris, France, 2004. 762–766
9 Takeshita O Y. A compact construction for LDPC codes using permutation polynomials. In: ISIT 2006. Seattle, USA, 2006. 79–82
10 O'Sullivan M E. Algebraic construction of sparse matrices with large girth. IEEE Trans Inf Theory, 2006, 52: 718–727
11 Milenkovic O, Kashyap N, Leyba D. Shortened array codes of large girth. IEEE Trans Inf Theory, 2006, 52: 3707–3722
12 Tao X F, Kim J M, Liu W Z, et al. Improved construction of low-density parity-check codes based on lattices. In: ISITC2007, Jeonju, Korea, 2007. 208–212
13 Zhang F, Mao X H, Zhou W Y, et al. Girth-10 LDPC codes based on 3-D cyclic lattices. IEEE Trans Veh Techn, 2008, 57: 1049–1060
14 Wu X F, You X H, Zhao C M. A necessary and sufficient condition for determining the girth of quasi-cyclic LDPC codes. IEEE Trans Comm, 2008, 56: 854–857
15 Wang Y, Yedidia J S, Draper S C. Construction of high-girth QC-LDPC codes. In: 5th Int Symp Turbo Codes Rel Top, Lausanne, Switzerland, 2008. 180–185
16 Liu L, Zhou W Y. Design of QC-LDPC code with continuously variable length (in Chinese). J El Inf Tech, 2009, 31: 2523–2526
17 Feng D G, Pei D Y. Relationship between two kinds of Chrestenson spectra over ring Z_N. Chinese Sci Bull, 1996, 41: 1494–1494
18 Zhang W Y, Wu C K, Liu X Z. Construction and enumeration of Boolean functions with maximum algebraic immunity. Sci China Ser F: Inf Sci, 2009, 52: 32–40
19 Guo B A. Generating and counting a class of binary bent sequences which is neither bent-based nor linear-based. Chinese Sci Bull, 1992, 37: 517

20 Guo B A. Construction of a class of binary sequences with two-valued autocorrelation. Chinese Sci Bull, 1993, 38: 873–873
21 Tong X J, Cui M G. Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation. Sci China: Inf Sci, 2010, 53: 191–202
22 Chen S, Zhong X X, Wu Z Z. Chaos block cipher for wireless sensor network. Sci China Ser F: Inf Sci, 2008, 51: 1055–1063
23 Sun Q. A kind of good elliptic curve used to set up cryptosystem. Chinese Sci Bull, 1990, 35: 81–81
24 Dong X L, Cao Z F. New designing of cryptosystems based on quadratic fields. Sci China Ser F: Inf Sci, 2008, 51: 1106–1116
25 Li D X. How to break up modified Lu-Lee cryptosystems. Chinese Sci Bull, 1991, 36: 1050
26 Li D X. Breaking a class of public-key cryptosystems with Euclid algorithm. Chinese Sci Bull, 1991, 36: 873
27 Luo P, Zhou H J, Wang D S, et al. Cryptanalysis of RSA for a special case with d>e. Sci China Ser F: Inf Sci, 2009, 52: 609–616
28 Wei Y Z, Hu Y P. New related-key rectangle attacks on reduced AES-192 and AES-256. Sci China Ser F: Inf Sci, 2009, 52: 617–626
29 Zhou L, Li S Q. New direction for joint design of stream cipher and error-correcting codes–advance of research on fast correlation attack decoding algorithm (in Chinese). J U El Sci Techn China, 2009, 38: 555–561
30 Fossorier M P C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. IEEE Trans Inf Theory, 2004, 50: 1788–1793
31 Liu Y H, Wang X M, Chen R W, et al. Generalized combining method for design of quasi-cyclic LDPC codes. IEEE Comm Lett, 2008, 12: 392–394
32 Jiang X Q, Lee M H. Large girth quasi-cyclic LDPC codes based on the Chinese remainder theorem. IEEE Comm Lett, 2009, 13: 342–344
33 Chilappagari S K, Nguyen D V, Vasic B, et al. Girth of the Tanner graph and error correction capability of LDPC codes. In: Proc 46th Ann All Conf Comm, Contr Comp, Illinois USA, 2008, THC6. 3, 1238–1245

Supporting Information

Appendix I: Classification of all the 8-cycles in the three lines of *S*

The supporting information is available online at csb.scichina.com and www.springerlink.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.